Conseils de sécurité pour les organisations dont les employées et employés travaillent à distance

Mars 2024

ITSAP.10.016

Le travail à distance pose certaines difficultés lorsqu'il s'agit de trouver un équilibre entre fonctionnalité et sécurité. Lorsqu'ils travaillent à distance, vos employées et employés doivent avoir accès aux services, aux applications et à l'information internes dont ils se serviraient normalement s'ils travaillaient depuis le bureau. Cependant, votre organisation doit également protéger ses systèmes et son information, étant donné que le travail à distance comporte sa part de risques. Vous devez donc mettre en place des mesures de sécurité additionnelles visant à empêcher les auteures et auteurs malveillants d'exploiter d'éventuelles vulnérabilités de vos

Comprendre les menaces pour les travailleuses et travailleurs à distance

Le travail à distance peut accroître le risque de compromission de l'information sensible de votre organisation. Les auteures et auteurs malveillants ont recours à diverses approches pour cibler les travailleuses et travailleurs à distance.

- **Accès physique à un dispositif :** Lorsqu'ils sont laissés sans surveillance dans un lieu public, les dispositifs peuvent être volés ou piratés par une auteure ou un auteur malveillant.
- **Hameçonnage :** Une auteure ou un auteur malveillant se faisant passer pour la représentante ou le représentant d'une organisation légitime communique avec la personne ciblée par courriel, par messagerie texte ou par téléphone pour lui demander de transmettre de l'information sensible, comme des mots de passe ou des numéros de cartes de crédit.
- **Piratage psychologique :** Une auteure ou un auteur malveillant peut collecter de l'information en ligne sur votre organisation ou sur une ou un membre de son personnel dans le but de créer un message d'hameçonnage qui paraît légitime.
    - Toute information publiée en ligne peut être utilisée, qu'elle provienne d'un site Web de l'organisation ou d'un compte personnel de médias sociaux.
- **Rançongiciel** : Une auteure ou un auteur malveillant utilise un maliciel pour empêcher une victime d'accéder aux données contenues dans son propre dispositif. Ensuite, cette auteure ou cet auteur ne permettra à la victime d'accéder à ses propres données que si elle lui verse une somme d'argent.
- **Piratage de réseau sans fil :** Une auteure ou auteur de menace crée un réseau sans fil malveillant, mais lui donne le nom d'un réseau existant et légitime, par exemple le nom du réseau public d'une chaîne de cafés-restaurants bien connue.
- **Écoute clandestine :** Une auteure ou un auteur malveillant surveille le trafic de réseaux sans fil et enregistre les activités en ligne ainsi que les mots de passe utilisés.
- **Altération du trafic** : Lorsqu'un dispositif mobile est infecté par du code trafiqué, une auteure ou un auteur malveillant peut y introduire du trafic piraté dans le but de fausser des données et d'accéder au réseau de votre organisation.

Gérer les dispositifs mobiles

Si possible, vos employées et employés devraient utiliser des dispositifs fournis par l'organisation lorsqu'ils travaillent à distance. Rappelez à vos employées et employés de suivre les politiques organisationnelles et d'utiliser les dispositifs selon les règles établies.

Lorsque les employées et employés utilisent des dispositifs personnels pour le travail, il faut être au courant des risques :

Omission d'installer les mises à jour de sécurité : Les dispositifs personnels peuvent ne pas être mis à jour ni corrigés régulièrement. Dans ce cas, les vulnérabilités persistent et accroissent les risques de compromission.

Utilisation de mots de passe faibles : Certains dispositifs personnels ne sont pas protégés par un NIP ni par un mot de passe. Et encore, l'emploi de NIP ou de mots de passe faibles (faciles à deviner) constitue un risque.

Perte de contrôle sur l'information : S'ils sont utilisés à des fins professionnelles, les dispositifs personnels peuvent contenir de l'information commerciale sensible que votre organisation ne peut plus gérer convenablement.

Rappelez aux employées et employés de suivre les politiques organisationnelles lorsqu'ils utilisent des dispositifs personnels. Le cas échéant, rappelez-leur les pratiques exemplaires qui permettent de sécuriser les dispositifs. Par exemple, veillez à ce que les employées et employés activent l'authentification multifacteur, utilisent des logiciels antivirus et ne laissent jamais les dispositifs sans surveillance dans un lieu public. Pour en apprendre davantage, reportez-vous à la publication Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)

Préparer votre effectif

Pour les employées et employés qui n'ont jamais travaillé à distance, la transition pourrait s'avérer difficile. Donnez-leur les moyens de bien s'adapter en leur communiquant clairement les mesures à prendre pour contribuer à la cybersécurité de votre organisation.

- Mettez en place des politiques et des procédures qui décrivent, par exemple, les modes acceptables d'utilisation des dispositifs organisationnels et de gestion de l'information de l'organisation.
- Veillez à ce que vos employées et employés sachent qui contacter, en particulier s'ils rencontrent des problèmes de sécurité ou si leur dispositif est égaré ou volé.

Formez vos employées et employés sur les enjeux de cybersécurité et sur les pratiques exemplaires, notamment :

- la détection des tentatives d'hameçonnage,
- la création de phrases de passe et de mots de passe forts,
- l'utilisation d'un réseau sans fil sécurisé.

SÉRIE SENSIBILISATION

No de cat. D97-1/10-016-2024F-PDF
ISBN 978-0-660-70531-6

Utiliser des outils de sécurité

Il existe des outils de sécurisation que votre organisation peut utiliser pour ajouter des couches de protection additionnelles à vos réseaux, systèmes et dispositifs. Or, les outils de sécurité peuvent réduire les risques pour votre organisation, mais il ne faut pas oublier qu'aucun outil n'est parfait. Vous ne devez jamais vous fier uniquement à un seul outil. Il faut également mettre en place des contrôles de sécurité complémentaires.

Les outils de sécurité présentés ci-dessous ne sont que quelques exemples des moyens que vous pouvez utiliser pour réduire les risques d'intrusions malveillantes causées par des maliciels ou par d'autres types de cyberattaques.

Réseau privé virtuel

Un réseau privé virtuel (RPV) est un tunnel de communication sécurisé et chiffré par lequel l'information est acheminée. Vous pouvez utiliser un RPV pour établir une connexion sécurisée qui impose un mode d'authentification et protège les données. L'utilisation d'un RPV permet d'assurer que les communications de votre organisation demeurent privées à travers un réseau non sécurisé. Indiquez à votre personnel qu'il est tenu d'utiliser le RPV pour se connecter aux serveurs de l'organisation.

Pare-feu

Un pare-feu est une barrière de sécurité placée entre deux réseaux. Il contrôle la quantité et les types de trafic qui peuvent circuler entre les réseaux. Un pare-feu renforce la sécurité des systèmes de l'organisation en surveillant le trafic entrant et le trafic sortant tout en filtrant le trafic indésirable que les systèmes peuvent reconnaître.

Logiciel antivirus

Vous devriez avoir recours à un antivirus et veiller à ce que celui-ci soit tenu à jour. Le logiciel antivirus protège les dispositifs contre les maliciels en balayant les fichiers et votre système.

Liste d'applications autorisées

Les listes d'applications autorisées permettent de contrôler les applications autorisées à s'exécuter sur des dispositifs organisationnels. Ainsi, votre organisation peut créer une liste d'applications autorisées qui définit toutes les applications approuvées et qui empêche les utilisatrices et utilisateurs d'exécuter ou d'installer des logiciels non autorisés sur les dispositifs organisationnels.

Remplacer les dispositifs en fin de vie

Les dispositifs qui ont atteint leur fin de vie représentent un risque pour la sécurité de votre organisation. La fin de vie signifie que le fournisseur cesse la commercialisation, la vente et le soutien technique ainsi que les mises à jour du dispositif. Lorsque vous utilisez des dispositifs sur lesquels les plus récentes mises à jour de progiciels n'ont pas été appliquées, vous vous exposez à des cyberattaques.

Un progiciel est un logiciel qui a été installé et mis à jour par le fabricant, et qui contient d'importantes mesures de sécurité. Vous pouvez vérifier si votre dispositif est en fin de vie en consultant la liste de produits en fin de vie du fournisseur ou en accédant aux dossiers du routeur dans les journaux du système.

Remplacer les dispositifs en fin de vie

Les dispositifs qui ont atteint leur fin de vie représentent un risque pour la sécurité de votre organisation. La fin de vie signifie que le fournisseur cesse la commercialisation, la vente et le soutien technique ainsi que les mises à jour du dispositif. Lorsque vous utilisez des dispositifs sur lesquels les plus récentes mises à jour de progiciels n'ont pas été appliquées, vous vous exposez à des cyberattaques.

Un progiciel est un logiciel qui a été installé et mis à jour par le fabricant, et qui contient d'importantes mesures de sécurité. Vous pouvez vérifier si votre dispositif est en fin de vie en consultant la liste de produits en fin de vie du fournisseur ou en accédant aux dossiers du routeur dans les journaux du système.

Protéger les dispositifs

Lorsque les employées et employés doivent travailler depuis leur domicile ou un lieu public, il devient important que les mesures énoncées ci-dessous soient rigoureusement appliquées pour protéger les dispositifs et leur information. Il conviendra également d'inciter les employées et employés à appliquer les mêmes mesures à leurs dispositifs personnels.

- **Utilisez l'authentification multifacteur :** Pour ajouter une couche de protection supplémentaire, imposez l'authentification à deux facteurs (ou plus) pour le déverrouillage des dispositifs. Par exemple, les facteurs d'authentification peuvent être un NIP et une empreinte digitale.
- **Utilisez des économiseurs d'écran activés par mot de passe :** Lorsqu'une utilisatrice ou un utilisateur est inactif, son dispositif se verrouille automatiquement après un laps de temps prédéfini.
- **Désactivez les fonctions Bluetooth et sans fil sur les dispositifs non utilisés :** La désactivation des fonctions Bluetooth et sans fil empêche les auteures et auteurs malveillants de se connecter aux dispositifs.
- **Mettez à jour vos systèmes et appliquez les correctifs :** Configurez les dispositifs pour qu'ils exécutent automatiquement la mise à jour des logiciels d'exploitation, des applications principales et des logiciels de sécurité. Vérifiez que le matériel est toujours pris en charge.

Protégez l'information

Votre organisation est tenue de protéger l'information sensible qu'elle collecte et utilise. Rappelez-vous que l'information sensible est une cible très prisée par les auteures et auteurs malveillants.

- **Sauvegardez l'information :** L'information doit être sauvegardée régulièrement, et les copies de sauvegarde doivent être conservées en toute sécurité.
- **Chiffrez l'information :** Utilisez les fonctions de chiffrement pour protéger la confidentialité de l'information sensible. Par exemple, vous devez autoriser les utilisatrices et utilisateurs à accéder uniquement à des sites Web compatibles HTTPS depuis les dispositifs de l'organisation.
- **Appliquez le principe du droit d'accès minimal :** Veillez à ce que les employées et employés aient accès seulement à l'information dont ils ont besoin pour accomplir leurs tâches. Ce type de contrôle peut prévenir les accès non autorisés aux données ainsi que les violations de données.

Pour en savoir plus

Les conseils énoncés plus haut constituent un bon point de départ. Pour en apprendre davantage, consultez certaines de nos publications connexes :

- Protéger votre organisation contre les maliciels (ITSAP.00.057)
- Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)
- Les réseaux privés virtuels (ITSAP.80.101)
- Piratage psychologique (ITSAP.00.166)
- Rançongiciels : comment les prévenir et s'en remettre (ITSAP.00.099)
- Pratiques exemplaires en matière de cybersécurité pour les routeurs (ITSAP.80.019)
- Produits obsolètes (ITSAP.00.095)